

Reporting Requirements and Examples

If you are unsure of what you are required to report, contact your FSO or security point of contact. When in doubt, report an event or behavior to your FSO or security point of contact.

What to Report

Reportable suspicious cyber incidents include, but are not limited to:

- System Failure or Disruption
- Suspicious Questioning
- Unauthorized Access
- Unauthorized Changes
- Suspicious Emails
- Unauthorized Use

Reporting Requirements for Contractor Personnel

Contractor Reporting Requirements for Cyber Intrusions (NISPOM 1-301)

Source: Industrial Security Letter 2013-05, July 2, 2013

Certain cyber intrusions into classified systems fall under the reporting requirement of NISPOM 1-301 and must be reported to the FBI, with a copy to DSS. Contractors must report activities that otherwise meet the threshold for reporting, including activities that may have occurred on its unclassified information systems.

Specifically, contractors must report cyber intrusions against classified information systems that may indicate:

- Espionage
- Sabotage
- Terrorism
- Subversive activity

A cyber intrusion reportable under NISPOM 1-301 may involve one or more of a combination of active efforts, such as:

- Port and services scanning from consistent or constant addresses
- Hacking into the system
- Placing malware hacking tools into the system
- Passive efforts (e.g., unsolicited emails containing malware or internet sites that entice users to download files that contain embedded malware)
- Exploitation of knowledgeable persons through “phishing” and “social engineering”

Contractors should consider the following guidelines when making a determination to report a cyber intrusion to the FBI and to DSS under NISPOM paragraph 1-301:

- Evidence of an advanced persistent threat
- Evidence of unauthorized exfiltration or manipulation of information
- Evidence of preparation of contractor systems or networks for future unauthorized exploitation
- Activity that appears to be out of the ordinary, representing more than nuisance incidents
- Activities, anomalies, or intrusions that are suspicious and cannot be easily explained as innocent

Contractors are also reminded they are required to report to DSS:

- Efforts by any individual, regardless of nationality, to “obtain illegal or unauthorized” access to an information system processing classified information (NISPOM paragraph 1-302b)
- “Significant vulnerabilities” identified in information system “hardware and software used to protect classified material” (NISPOM paragraph 1-302j)

Contractors should also report cyber intrusions into unclassified information systems if the contractor determines they meet the following conditions:

- “(i) the facts and circumstances of the intrusion are sufficient to qualify as actual, probable, or possible espionage, sabotage, terrorism, or subversive activities,”

- and “(ii) these activities constitute a threat to the protection of classified information, information systems, or programs that are otherwise covered by the NISPOM.” (ISL 2013-05 July 2, 2013)

Note: Many attempts to gather classified information as well as attempts to gain access to classified information systems begin on unclassified networks. Through use of social engineering, deployment of malware, and/or the aggregation of information available on unclassified systems, adversaries are able to derive classified data and even the tools used to target classified information systems.

Reporting Requirements for DoD Personnel

DoD Reportable Foreign Intelligence Entity (FIE)-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors

Source: DoDD 5240.06, May 17, 2011 Incorporating Change 1, May 30, 2013

DoD personnel who fail to report the contacts, activities, indicators, and behaviors in items 1-10 are subject to punitive action.

1. Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.
2. Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.
3. Network spillage incidents or information compromise.
4. Use of DoD account credentials by unauthorized parties.
5. Tampering with or introducing unauthorized elements into information systems.
6. Unauthorized downloads or uploads of sensitive data.
7. Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.
8. Downloading or installing non-approved computer applications.
9. Unauthorized network access.
10. Unauthorized e-mail traffic to foreign destinations.

The indicators in items 11-19 are reportable, but failure by DoD personnel to report these indicators may not alone serve as the basis for punitive action.

11. Denial of service attacks or suspicious network communications failures.
12. Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.
13. Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.
14. Data exfiltrated to unauthorized domains.
15. Unexplained storage of encrypted data.
16. Unexplained user accounts.
17. Hacking or cracking activities.
18. Social engineering, electronic elicitation, e-mail spoofing or spear phishing.
19. Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers